LATHAM & WATKINS LLP
Melanie M. Blunschi (Bar No. 234264)
melanie.blunschi@lw.com
Kristin Sheffield-Whitehead (Bar No. 304635)
kristin.whitehead@lw.com
505 Montgomery St., Suite 2000
San Francisco, CA 94111
Telephone: +1.415.391.0600

Andrew B. Clubok (*pro hac vice*)
andrew.clubok@lw.com
555 Eleventh Street, NW, Suite 1000
Washington, D.C. 20004
Telephone: +1.202.637.2200

Michele D. Johnson (Bar No. 198298)
michele.johnson@lw.com
650 Town Center Drive, 20th Floor
Costa Mesa, CA 92626
Telephone: +1.714.540.1235

Attorneys for Defendant Meta Platforms, Inc. (formerly known as Facebook, Inc.)

[Additional Counsel Listed Below]

ELIZABETH K. MCCLOSKEY (SBN 268184)
EMcCloskey@gibsondunn.com
ABIGAIL A. BARRERA (SBN 301746)
ABarrera@gibsondunn.com
One Embarcadero Center, Suite 2600
San Francisco, CA 94111-3715
Telephone: 415.393.8200
Facsimile: 415.393.8306

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

SAN FRANCISCO DIVISION

ERICA FRASCO et al.,

Plaintiffs,

v.

FLO HEALTH, INC., GOOGLE LLC, FACEBOOK, INC., and FLURRY, INC.,

Defendants.

CASE NO. 3:21-CV-00757-JD (consolidated)

DEFENDANT META PLATFORMS, INC.'S REPLY IN SUPPORT OF MOTION FOR SUMMARY JUDGMENT

Judge: Hon. James Donato
Court: Courtroom 11 – 19th Floor
Date: April 24, 2025
Time: 10:00 a.m.

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Page(s)

Cases

TABLE OF AUTHORITIES
(Cont'd.)

Page(s)

TABLE OF AUTHORITIES
(*Cont'd.*)

Page(s)

Statutes

INTRODUCTION

Plaintiffs' opposition confirms the Court should grant summary judgment to Meta because they cannot prove essential elements of their Wiretap Act, CIPA, CDAFA, UCL, and aiding-and-abetting claims. Plaintiffs concede their UCL claims should be "dismiss[ed]." Opp. 25. As for their other claims, plaintiffs misstate the law, mischaracterize the evidence to manufacture a factual dispute when there is none, or both. Flo's decision to create, name, and send the challenged "Custom Events" directly to Meta cannot subject Meta to liability, and a contrary conclusion would be akin to punishing someone for opening mail addressed to her and delivered to her own mailbox.

Wiretap Act and CIPA claims. Plaintiffs cannot prevail on their Wiretap Act and CIPA claims for four independent reasons. First, plaintiffs indisputably were not parties to the communications they challenge; only Meta and Flo were. The undisputed evidence shows Flo decided to incorporate Meta's SDK into the Flo app, created the challenged Custom Events, and sent those Events—which differed from what users entered into the app—to Meta. None of plaintiffs' evidence suggests otherwise. Plaintiffs' Figure 2 shows the many steps that the *Flo app code* took before the Custom Events were even created and sent to Meta. Opp. 4. Because plaintiffs were never parties to the communications between Meta and Flo, those communications cannot be the basis of any wiretapping or eavesdropping claims. And as a party to those communications, Meta cannot be held liable for receiving them from Flo, and there is no evidence Meta received them for some criminal or tortious purpose.

Second, Meta did not "intercept" any Custom Events while they were "in transit," as required under the Wiretap Act and CIPA § 631(a). Instead, plaintiffs' opposition and their expert's analysis confirm that the Custom Events were not even created by the Flo app code until after users finished taking a certain action, and that the Events were then stored on users' devices before Flo sent them to Meta. Under binding Ninth Circuit law, that is not an "interception" of a communication "in transit."

Third, none of plaintiffs' evidence shows Meta "intended" to "intercept" or "eavesdrop" on their health communications. To the contrary, their cited evidence only underscores that Meta would never have received the Custom Events but-for Flo's actions and that Meta never wanted to receive health information, which its terms prohibited Flo and other developers from sending through its SDK.

Fourth, plaintiffs and Flo consented to the data sharing. Plaintiffs agreed as Facebook users,

and Flo consented by sending Meta the data. Plaintiffs do not dispute Flo consented, and instead argue they did not consent to the data sharing because Flo's privacy policies purportedly said their health information would not be shared and because Meta's privacy policies were too general. But a separate contract with Flo cannot alter the terms of Meta's contract with plaintiffs, and the Ninth Circuit squarely rejected both of plaintiffs' arguments in *Smith v. Facebook, Inc.*, 745 F. App'x 8 (9th Cir. 2018).

CDAFA claim. Plaintiffs cannot prevail on their CDAFA claim because Meta did not "knowingly" or "actively" participate in any "hacking" under the CDAFA, plaintiffs consented to any "hacking," and plaintiffs did not suffer the requisite "damage or loss" under the statute. In response, plaintiffs claim the fact that Meta made its SDK publicly available to app developers is sufficient to demonstrate it "knowingly" and "actively" participated in "hacking," but there is no authority supporting that position. And although plaintiffs now claim they lost the value of their data, none of them identified that harm during their depositions, and regardless, the vast majority of courts to reach the issue have held that type of harm insufficient to support a claim under the CDAFA.

Aiding-and-abetting claim. None of plaintiffs' cited evidence shows Meta knew about Flo's allegedly deceptive disclosure practices, let alone that Meta substantially assisted in those practices. And again, plaintiffs' consent bars this claim.

ARGUMENT

I. Plaintiffs Cannot Prove Essential Elements Of Their Wiretap Act And CIPA Claims

A. Meta Did Not "Intercept" or "Eavesdrop" On Plaintiffs' Communications.

To prevail on their wiretapping and eavesdropping claims, plaintiffs must prove Meta "intercepted" or "eavesdropped" on their communications. Mot. 8–12. Plaintiffs therefore need evidence that Meta took information intended for Flo. But the record shows that never happened. Plaintiffs sent information to Flo, and then Flo later sent different information altogether, the challenged Custom Events, directly to Meta. Receiving information that was intended for Meta and that was different from what plaintiffs told Flo is neither an "interception" nor "eavesdropping."

1. The Communications At Issue Were Between Flo and Meta.

There is no dispute plaintiffs must prove Meta intercepted and eavesdropped on *their* communications. Mot. 8–9. There is also no genuine factual dispute plaintiffs were never *parties* to

the communications at issue, i.e., the Custom Events. Instead, only Flo and Meta were parties to those communications, which were separate and distinct from plaintiffs' communications with the Flo app.

Specifically, the undisputed evidence shows *Flo* programmed its app code to generate the Custom Events it sent to Meta, and those Events included information that was different from what plaintiffs entered into the app. Mot. 4–5. There is no dispute that plaintiffs had no involvement in the Flo app code's creation of the Custom Events. Plaintiffs concede as much, agreeing their expert's "testing [of the Flo app] show[ed] *Flo sent* the [Custom App] events as well as [their] parameter[s] . . . *to Meta*." Opp. 13–14 (emphasis added) (contradicting their argument that "Flo does not transmit anything to Meta"). And there is no evidence the plaintiffs even saw the Custom Events that Flo generated and sent to Meta until this litigation, let alone that they were parties to those communications.

Take R_SELECT_LAST_PERIOD_DATE, which plaintiffs' expert claims was sent with the parameter "known" or "unknown"—not the date someone entered into the Flo app. Mot. 5. That parameter was generated by the Flo app, was named by Flo, and did not contain or bear any resemblance to the user's communication with the app. *Id.* 4–5. The same is true of R_SELECT_PERIOD_LENGTH, which plaintiffs' expert also claims was sent with a parameter of "known" or "unknown"—not the period length someone entered into the app. Mot. 9. Plaintiffs' expert's testing confirmed that the information users communicated to Flo and the data that Flo generated and sent to Meta "differ[]" and "were not duplicative." App. 720–23. And while plaintiffs say their expert never actually said those words (Opp. 14 n.8), that is irrelevant: Meta's point is that his "analysis *showed*" those points were true, demonstrating there is no genuine dispute on this (Mot. 11 (emphasis added)).

Plaintiffs' opposition is silent on R_SELECT_LAST_PERIOD_DATE, R_SELECT_PERIOD_LENGTH, and almost all the other challenged Custom Events. Instead, they focus on just one of the 12 challenged Custom Events, R_CHOOSE_GOAL, claiming the parameter that was sent with that event was similar to what users entered into the Flo app. *See* Opp. 3–4, 14. But the facts as plaintiffs describe them establish that R_CHOOSE_GOAL and its parameter followed the same exact technical process as the other Custom Events: Plaintiffs claim users first selected a button responding to the question "How can we help you?" with a response of, for instance, "I just want to track my cycle." Opp. 4 (Figure 2). Even according to plaintiffs, after the user made that selection, the same

cascade of processing steps then occurred within the Flo app code, including its creation of the string that included a Custom Event titled R_CHOOSE_GOAL and a text parameter "track_cycle." *Id.*; *see also id.* 14 (plaintiffs' expert's testing "show[ed]" "Flo received users' survey responses," after which "Flo sent the R_CHOOSE_GOAL event as well as its parameter . . . to Meta"). That Flo's programming resulted in the creation of parameters similar to the substance of a user's communication with Flo in this one instance does not change the undisputed technical process here, which makes clear that the Flo app code generated these communications, that plaintiffs were not involved in that process, and that Meta was a party to those communications as Flo's intended recipient. Mot. 4–5.

The undisputed evidence, then, shows the challenged Custom Events are separate communications with Meta created *after* the plaintiffs finished taking certain actions with the Flo app—that is, there was no "interception" of what plaintiffs sent to Flo. Plaintiffs appear to suggest Meta must be liable because those separate Flo-to-Meta communications (of different information) relate to initial plaintiffs-to-Flo communications. But that theory would not work even if the content of the communications were *identical*. "[A] substantial distinction has been recognized between the secondhand repetition of the contents of a conversation and its simultaneous dissemination to an unannounced second auditor." *Smith v. LoanMe, Inc.*, 11 Cal. 5th 183, 200 (2021); *see also Flanagan v. Flanagan*, 27 Cal. 4th 766, 775 (2002) (same); *Brodsky v. Apple Inc.*, 445 F. Supp. 3d 110, 127 (N.D. Cal. 2020) ("The analysis for a violation of CIPA is the same as that under the federal Wiretap Act."). Here, the undisputed facts show the Custom Events were not the same as plaintiffs' communications with the app, and any similarity between the Custom Events and plaintiffs' communications with the Flo app would be, at most, nonactionable "secondhand repetition." Mot. 4–5, 9; Opp. 3–4.

In a final effort to support their "interception" theory, plaintiffs accuse Meta of not citing "authority supporting its position that the [Custom Events] . . . are communications between Flo and Meta" (Opp. 12), but that is not a legal argument; it is instead an undisputed fact about how the technology at issue in this case works. The technology worked differently in the cases plaintiffs cite. *In re Facebook, Inc. Internet Tracking Litigation*, 956 F.3d 589 (9th Cir. 2020), and *In re Pharmatrak, Inc.*, 329 F.3d 9, 22 (1st Cir. 2003), both involved technology that caused the defendant to receive communications "identical" to and "simultaneous" with the plaintiffs' communications with their

intended recipient. Plaintiffs have not cited any evidence showing the same is true here. Opp. 14 (citing Dkt. 478-10 ¶ 20 (does not show Flo received Custom Events); Dkt. 478-6 ¶ 69 (claiming Flo "calculated" certain information "based on" users' inputs); Dkt. 478-6 ¶ 86 (showing only what Meta purportedly received); Dkt. 478-6 ¶ 76 Fig. 13 (showing only what "data was transmitted to [a defendant's] servers")); *see also* App. 721–22. The remainder of plaintiffs' cases are also unhelpful because no argument was raised in those cases about whether the plaintiffs were parties to the at-issue communications, or those courts had to accept the plaintiffs' allegations as true, and/or those cases involved materially different technologies. *See* Dkt. 485 at 6–7 (no argument plaintiffs were not parties to Custom Events); *In re Zynga Priv. Litig.*, 750 F.3d 1098, 1107 (9th Cir. 2014) (similar); *Gladstone v. Amazon Web Servs., Inc.*, 739 F. Supp. 3d 846, 854 (W.D. Wash. 2024) (same); *Valenzuela v. Nationwide Mut. Ins. Co.*, 686 F. Supp. 3d 969, 979 (C.D. Cal. 2023) (court accepted as true allegation that defendant's "code intercepts chat messages in real time and stores transcripts").

In short, plaintiffs' argument that they were parties to the communications because what they entered into the Flo app was "acquired" by "Meta's SDK" (Opp. 11–12, 14) is belied by the undisputed record. Plaintiffs' communications with Flo concluded before the Flo app code generated different data (the Custom Events) and then sent them to Meta. *See supra* 2–3.[1]

2. Meta Cannot "Wiretap" Or "Eavesdrop" On Itself.

Even if plaintiffs were parties to the communications at issue, Meta could not be liable for "wiretapping" or "eavesdropping" on those communications under the "party exception" because Meta indisputably was also a party to those communications. Mot. 10–11.

CIPA §§ 631(a) and 632. "Courts perform the same analysis for both the Wiretap Act and CIPA regarding the party exemption." *Internet Tracking*, 956 F.3d at 607. And under both CIPA and the federal Wiretap Act, "a person who is a 'party' to the communication" cannot be liable for "intercept[ing]" it. *Id.* at 607. Plaintiffs misstate the law by suggesting the party exception is limited to instances where "third parties who intercept data . . . function as a mere 'tape recorder' for one of

[1] Plaintiffs' suggestion that Meta's SDK operates separate and apart from the Flo app is contrary to the evidence in this case (*see, e.g.*, App. 713–15 (explaining SDK code "becomes a part of" an app that then runs "as a single cohesive application")), but even if one accepted their version of events for the purposes of this motion only, Meta's above-described arguments would still stand.

the parties to the communication," citing a single case. Opp. 15–16 (citing *Turner v. Nuance Commc'ns, Inc.*, 735 F. Supp. 3d 1169, 1182 (N.D. Cal. 2024)). Courts regularly dismiss CIPA claims alongside Wiretap Act claims under the party exception, applying the same party-exception analysis with no reference to a "tape recorder" limitation. *See, e.g.*, *B.K.v. Eisenhower Med. Ctr.*, 721 F. Supp. 3d 1056, 1065–66 (C.D. Cal. 2024) (dismissing federal Wiretap Act and CIPA § 631 claim); *Pena v. GameStop, Inc.*, 670 F. Supp. 3d 1112, 1118–20 (S.D. Cal. 2023) (same); *Gonzales Uber Techs., Inc.*, 305 F. Supp. 3d 1078, 1089 (N.D. Cal. 2018) (dismissing CIPA § 632 claim). Plaintiffs' cited case does not hold otherwise. There, the plaintiffs brought CIPA claims, claiming their phone calls with their bank were recorded by the defendant's software. *Turner*, 735 F.3d at 1175. The defendant claimed it was not a third party to those calls "because [it] only provided a tool that [the bank] used for its own purposes." *Id.* at 1182. There, the question before the court was whether the defendant's product was a mere "tool" or did more, and the court concluded it did more. But Meta does not argue it provided a "tool" to record users' communications with Flo; instead, the undisputed facts establish there were only two parties (Flo and Meta) to the at-issue communications, and Meta was the intended recipient of those communications. That is why imposing liability here would be akin to punishing someone for opening mail that was addressed and delivered to her own mailbox. Mot. 10–11.

Federal Wiretap Act. Plaintiffs agree that parties to communications cannot be liable under the federal Wiretap Act (the "party exception") but argue the exception does not apply because Meta purportedly acted "for the purpose of committing a[] criminal or tortious act" (the "crime-tort exception"). 18 U.S.C. § 2511(2)(d); *see* Opp. 14–15. But the crime-tort exception requires proof that Meta acted "with criminal and/or tortious intent," and it applies only when the "criminal or tortious act" is "independent of the intentional act of . . . interception itself." *B.K.*, 721 F. Supp. 3d at 1065. "[T]he focus is not upon whether the interception itself violated another law; it is upon whether the *purpose* for the interception—its intended use—was criminal or tortious." *Sussman v. Am. Broad. Cos.*, 186 F.3d 1200, 1202 (9th Cir. 1999). Plaintiffs' single cited case (Opp. 14) is in agreement. *See R.S. v. Prime Healthcare Servs., Inc.*, 2025 WL 103488, at *4 (C.D. Cal. Jan. 13, 2025).

Here, too, plaintiffs focus solely on the claimed interception itself. Plaintiffs argue "Flo and Meta wanted to disclose Plaintiffs' private health data" and "sought to . . . use [the data] for their own

commercial benefit," and that this conduct "violates several laws," naming CMIA, CDAFA, and HIPAA. Opp. 14–15. But plaintiffs' "own argument demonstrates that the alleged tortious or criminal use of the acquired communications *is the disclosure itself*." *Nienaber v. Overlake Hosp. Med. Ctr.*, 2025 WL 692097, at *13 (W.D. Wash. Mar. 4, 2025) (dismissing wiretapping claims) (emphasis added); *see also, e.g.*, *B.K.*, 721 F. Supp. 3d at 1065 (similar); *In re Google Inc. Cookie Placement Consumer Privacy Litig.*, 806 F.3d 125, 145 (3d Cir. 2015) (similar). The court in *B.K.* dismissed the plaintiffs' wiretapping claims for this reason, explaining that although the defendant allegedly intercepted plaintiffs' information "for Defendant's commercial advantage," "Plaintiffs do not allege that this purpose constitutes independently illegal or actionable conduct." 721 F. Supp. 3d at 1065. The court did so even though those plaintiffs brought separate CMIA, privacy, and other claims based on the defendant's conduct—just as plaintiffs have done here. *Id.* at 1060.

Besides merely asserting Meta's conduct "violates" the CDAFA, CMIA, and HIPAA, plaintiffs do not explain how Meta's *purpose* in receiving plaintiffs' data violates those statutes separate and apart from the "interception" itself. Opp. 14–15. Plaintiffs have not asserted CMIA or HIPAA claims against Meta, and plaintiffs concede the crux of their CDAFA claim is based on the same underlying "interception." *See id.* at 22–23 (claiming Meta violated the CDAFA when it "'knowingly accesse[d]' [plaintiffs'] devices to obtain their private, in-app communications with Flo without their consent"). Further, courts have routinely held acting for commercial gain—what plaintiffs claim Meta has done here—is not a criminal or tortious purpose. *See, e.g.*, *Katz-Lacabe v. Oracle Am., Inc.*, 668 F. Supp. 3d 928, 945–46 (N.D. Cal. Apr. 6, 2023). As a result, the crime-tort exception does not apply, and Meta is entitled to summary judgment on plaintiffs' Wiretap Act claim under the party exception.

B. Meta Did Not Contemporaneously Intercept Plaintiffs' Communications.

Federal Wiretap Act. Plaintiffs do not dispute that Meta cannot be held liable under the Wiretap Act if it did not "intercept" the Custom Events when they were "in transit." *Konop v. Hawaiian Airlines, Inc.*, 302 F.3d 868, 878 (9th Cir. 2002). The Wiretap Act defines "intercept" to mean "acquisition of the contents of any wire, electronic, or oral communication." *Id.* at 876; Opp. 11 (same). "Such acquisition occurs 'when the contents of a wire communication are captured or redirected in any way,'" *Noel v. Hall*, 568 F.3d 743, 749 (9th Cir. 2009), and must happen "before [the communication's]

arrival" at storage—even "temporary, intermediate" storage, *Konop*, 302 F.3d at 878 & n.6.

Plaintiffs' opposition confirms there is no genuine factual dispute that Meta did not "initially acquir[e]" the Custom Events until *after* users finished taking certain actions within the Flo app. Specifically, while plaintiffs claim Meta's SDK "captured" Custom Events, even they agree the Custom Events are created, or "triggered," only *after* a user takes a certain action in the app. Opp. 3–4. This makes logical sense because, as their expert acknowledges, Custom Events are generated based on events that occur within the app, meaning users' actions necessarily must be complete before the Flo app code can generate the Custom Events. *See* Mot. 4–5; Opp. 3–4 (showing nearly half a dozen processing steps before Custom Events are generated); *see also, e.g.*, App. 576 (plaintiffs' expert claiming R_SELECT_LAST_PERIOD_DATE "indicate[d]" whether a user "*entered* the date of their last period" (emphasis added)). The Custom Events are then stored, or "cached," on the user's device *before* being "transmi[tted] . . . to Meta's servers." Opp. 4. As plaintiffs' expert admits, that storage may last for "seconds" or even "minutes" (App. 573–74, 620–21); however long it lasts, it still indisputably occurs before Meta "acquire[s]" the data. *Konop*, 302 F.3d at 878.[2]

Plaintiffs argue that because the Flo app's creation and transmission of Custom Events to Meta may take little time (e.g., milliseconds, seconds, or minutes), that process is "insignifican[t]" under the law (Opp. 17–18), but that theory contravenes the Ninth Circuit's clear guidance on the "narrow" definition of "interception." *Konop*, 302 F.3d at 878–79 & n.6. For example, interception after "any temporary, intermediate" storage is not actionable, regardless of how temporary the storage may be. *Id.* Based on the Ninth Circuit's guidance, courts in this district have routinely dismissed wiretapping claims based on the "in transit" requirement, even while acknowledging that the "window during which an interception may occur is exceedingly narrow" given "the almost instantaneous transmission of text messages." *Sunbelt Rentals, Inc. v. Victor*, 43 F. Supp. 3d 1026, 1031 (N.D. Cal. 2014); *see also Murray v. Fin. Visions, Inc.*, 2008 WL 4850328, at *6 (D. Ariz. Nov. 7, 2008) (similar). If the scope of the wiretapping statutes seems insufficiently narrow, it is up to Congress, not the courts, to "cover

[2] Plaintiffs point to their expert's characterization of the purported "interception[s]" as "contemporaneous" with when users entered data into the app (Opp. 16–18), but the parties agree on the technical process that results in the creation of Custom Events—and that process shows the data were not "intercepted" while "in transit."

the bases untouched." *Fraser v. Nationwide Mut. Ins. Co.*, 352 F.3d 107, 114 (3d Cir. 2003).

None of plaintiffs' cited cases helps them either. The courts there were required to accept the plaintiffs' allegations about the timing of interceptions as true, there was no argument raised about whether the "in transit" requirement was met, and/or the court's reasoning ran contrary to the Ninth Circuit's binding guidance in *Konop*. *See India Price v. Carnival Corp.*, 712 F. Supp. 3d 1347, 1359–60 (S.D. Cal. 2024) (motion to dismiss); *D'Angelo v. FCA US, LLC*, 726 F. Supp. 3d 1179, 1198 (S.D. Cal. 2024) (same); *Jones v. Peloton Interactive, Inc.*, 2024 WL 3315989, at *4 (S.D. Cal. July 5, 2024) (same, and no argument was raised regarding timing of interception); *In re Carrier IQ, Inc.*, 78 F. Supp. 3d 1051, 1081–82 (N.D. Cal. 2015) (ruling on motion to dismiss and incorrectly rejecting *Konop*'s holding regarding "temporary, intermediate" storage as "dicta").

CIPA § 631(a). With respect to their CIPA § 631(a) claim, plaintiffs argue they do not need to prove Meta "intercepted" communications while they were "in transit" and can instead prevail if "Meta 'received' and 'read' or 'learn[ed]' the contents' [of] these communications in California." Opp. 17. Courts have soundly rejected the "extraordinary breadth" of that interpretation of the statute. *Adler v. Community.com, Inc.*, 2021 WL 4805435, at *4 (C.D. Cal. Aug. 2, 2021) (holding CIPA § 631(a) requires proof "that the defendant 'read or learned the contents of a communication while the communication was in transit, or in the process of being sent or received' "); *see also, e.g.*, *Heiting v. Taro Pharms. USA, Inc.*, 728 F. Supp. 3d 1112, 1125 (C.D. Cal. 2024) ("Courts have repeatedly rejected . . . Plaintiff's argument that it is sufficient to allege that the communication was sent from, or received within California."). Even if the Court assumed for the sake of argument that plaintiffs' interpretation is correct, plaintiffs cannot rely on mere conclusory statements. Plaintiffs bore the burden of "go[ing] beyond the pleadings" to show "there is a genuine issue for trial," *Celotex Corp. v. Catrett*, 477 U.S. 317, 324 (1986), but they did not cite any evidence showing Meta "received," "read," or "learned the contents" of the Custom Events in California. Opp. 17 (discussing only "alleg[ations]").

C. There Is No Evidence Meta Intended To "Intercept" Or "Eavesdrop" On Plaintiffs' Communications.

Plaintiffs must prove Meta "acted consciously and deliberately with the goal of intercepting" their health communications with Flo. *United States v. Christensen*, 828 F.3d 763, 791 (9th Cir. 2015);

Mot. 13–16. Because no evidence shows Meta intended to intercept those communications, the Court should enter summary judgment on plaintiffs' Wiretap Act and CIPA claims.

Plaintiffs first argue they need only show that Meta intended to intercept *any* "event data," relying on *Christensen*. Opp. 19. But plaintiffs are not suing based on the interception of all "event data"; after all, no law prohibits the use of SDKs to collect data. *See* Dkt. 154 at 10:2-3 ("There is nothing unjust about using an SDK."). Designing an SDK to transmit Custom Events is thus not the same as designing it to be "primarily useful for the purpose of the surreptitious interception of . . . communications," as plaintiffs suggest. Opp. 19. Indeed, plaintiffs do not take issue with Flo's use of Meta's SDK generally; they argue only that Meta "intercepted" or "eavesdropped" on twelve Custom Events allegedly reflecting their "*health* data." Dkt. 64 ¶¶ 400, 410 (emphasis added); *see* Mot. 13–14. Plaintiffs must therefore prove Meta intended to intercept their health information. *See, e.g.*, *Doe I v. Google*, 741 F. Supp. 3d 828, 840–41 (N.D. Cal. July 22, 2024); Mot. 13–14.

Plaintiffs are wrong to suggest *Christensen* held otherwise. The issue there was whether the Wiretap Act "require[s] a defendant to know that his conduct is unlawful." 828 F.3d at 791. The Ninth Circuit held that knowledge was not required, because "the operative question under [the statute] is whether the defendant acted consciously and deliberately with the goal of intercepting wire communications." *Id.* Here, Meta is not arguing plaintiffs must prove it knew its conduct was unlawful. Rather, Meta is arguing plaintiffs must show it intended to "intercept" their health information, which is consistent with *Christensen*. Mot. 13–14. In a case similar to this one, Judge Chhabria applied *Christensen* and held the plaintiffs were required to allege the defendant "intentionally obtained" their "private health information." *Doe I*, 741 F. Supp. 3d at 840, 842 (dismissing wiretapping claim for this reason).

Plaintiffs next argue that, even if they are required to prove Meta intended to intercept their health information, there is "ample evidence demonstrating Meta knew it was collecting and using . . . health information from Flo." Opp. 19–20. But even a cursory review of plaintiffs' cited evidence reveals there is no genuine dispute that Meta never wanted to receive health information. Of the documents that plaintiffs cite that pre-date the close of the relevant period, only three even mention "health" information. *See* Dkt. 478-52. The rest do not mention "health" information and therefore

cannot show Meta "knew it was receiving *health* information from Flo," as plaintiffs suggest. Opp. 7 (emphasis added); *see* Dkt. 478-53 (addressing "sensitive user data" like "user PII" and "credit card number," not health information); Ps.' Ex. 12 (similar); Exs. 16–17 (concerning "App Events" generally); Exs. 18–19 (similar); Ex. 20 (discussing Meta and Flo's general business relationship).

The three documents that do reference "health" information also fail to demonstrate there is a factual dispute regarding Meta's intent. One suggests, at most, that it was *possible* app developers could "send sensitive information" to Meta, such as "health info"—not that Meta knew it was actually receiving such information, let alone from Flo. Dkt. 478-52. The document describes Meta's suggested response: "Systematically detect . . . and remove sensitive information from pixel, app and offline custom data and alert advertisers based on severity." *Id.* This document thus confirms Meta never wanted "health info" in the first place. The other two documents were sent at a time when (it is undisputed) Meta had implemented a system designed to detect and filter out "potential personally identifiable information [PII]" that may have been sent in violation of Meta's terms. App. at 164. These two documents are Meta's notices to Flo explaining the Flo app had "been identified as sending [Meta] data that may violate [its] Business Tools Terms" (that is, PII), reiterating what those terms prohibit, explaining that violative data "is removed from [Meta's] system," and advising Flo to "make sure you are only sending us data that complies with our Terms." Exs. 22–23. Flo's response to one of those notices included the assurance that it "do[es] not send any data that violates [Meta's] Business Tools Terms." Ex. 22. These documents do not establish that Meta was aware that Flo was sending health information, much less that it wanted that information; if anything, these documents show that when Meta became aware that Flo was potentially violating its terms by sending PII, it took action. It is also undisputed that Meta developed a system focused on detecting and filtering out "potential health information" after being alerted to allegations in the 2019 *Wall Street Journal* article. App. 164–65. Thus, these documents only underscore Meta's ongoing and evolving efforts to enforce its terms, and that Flo reassured Meta it was abiding by those terms. In fact, the other documents plaintiffs cite that do not mention health information similarly show Meta sought to ensure it did not receive other sensitive information. *See, e.g.*, Ex. 12 (Meta "eng[ineering] to build a filtering mechanism to detect [PII/sensitive data] and discard it").

As for the plaintiffs' cited documents that post-date the relevant period, those documents are even further afield. None of them suggests Meta intended to receive health information during the relevant period. *See, e.g.*, Ex. 10 (July 2020 document explaining the "aggressive" actions Meta will take "to mitigate the risk of violation" of their terms prohibiting receipt of health information).

In sum, the undisputed record demonstrates Meta expressly prohibited Flo from sending any "health" or "other sensitive information," and there is no evidence Meta wanted to "intercept" or "eavesdrop" on plaintiffs' health information. Meta should be granted summary judgment on plaintiffs' Wiretap Act and CIPA claims for this reason alone. *See Doe I*, 741 F. Supp. 3d at 840.

D. Plaintiffs' Claims Are Barred By Consent.

Plaintiffs' and Flo's consent to data sharing bars plaintiffs' wiretapping and eavesdropping claims. Mot. 16–19.[3] Plaintiffs do not dispute Flo's consent, so Meta is entitled to summary judgment on their Wiretap Act claim for that reason alone. Plaintiffs challenge only *their* consent, arguing their agreements with Flo somehow nullify their agreement with Meta, and that Meta's terms do not reflect consent because they do not reference the collection of health information. Opp. 20–22.[4] The Ninth Circuit rejected both arguments in *Smith v. Facebook*, 745 F. App'x 8 (9th Cir. 2018).

First, it is a fundamental principle of contract interpretation that "[a] contract must be interpreted so as to give effect to the mutual intention of the parties as it existed at the time of contracting, so far as ascertainable and lawful." Cal. Civ. Code § 1636. Moreover, only "[t]he language of a contract is to govern its interpretation, if the language is clear and explicit, and does not involve absurdity." *Id.* § 1638. In line with those fundamental principles, the Ninth Circuit has held plaintiffs cannot rely on their entirely separate contract with another party to evade the terms of their

[3] Contrary to plaintiffs' argument otherwise, plaintiffs bear the burden of proving Meta lacked consent under, for instance, CIPA, where lack of consent is an element of those claims. *See, e.g.*, *Reyes v. Educ. Credit Mgmt. Corp.*, 773 F. App'x 989, 990 n.1 (9th Cir. 2019) (noting plaintiff bears burden of proof under CIPA § 632); Cal. Penal Code §§ 631(a), 632(a).

[4] To the extent plaintiffs are now claiming Ms. Chen was a Facebook user during the relevant period (Opp. 22), then her claims are also barred by her consent to Meta's terms and policies. And although plaintiffs argue there is evidence "confirm[ing]" Meta "collected persistent identifiers associated with Plaintiff Chen" (*id.*), none of their cited evidence shows Meta could associate her with information it received from Flo if she was not a Facebook user. *See, e.g.*, App. 688–91 (explaining that the device information Meta received cannot be used to identify an individual).

contract with Meta. *See Smith*, 745 F. App'x at 9; *see also, e.g.*, *Van Ness v. Blue Cross of Cal.*, 87 Cal. App. 4th 364, 372 (2001) ("Where contract language is clear and explicit and does not lead to an absurd result, [courts] ascertain [the contracting parties'] intent from the written provisions and go no further."). In *Smith*, the plaintiffs claimed Meta had "collect[ed] and us[ed] their browsing data from various healthcare-related websites." 745 F. App'x at 8. The Ninth Circuit affirmed dismissal of the complaint, holding that "Plaintiffs consented to Facebook's data tracking and collection practices." *Id.* In doing so, the Ninth Circuit rejected the plaintiffs' argument that "Facebook could not have gained consent because the healthcare websites' privacy policies promised not to share data with third parties." *Id.* at 9. The Ninth Circuit reasoned that "Facebook's Terms and Policies make no such assurance, and *Facebook is not bound by promises it did not make*." *Id.* (emphasis added). The same reasoning applies here. Meta cannot be bound by Flo's representations to plaintiffs, whatever they were, and those representations cannot be used to alter the meaning of Meta's contract with plaintiffs.

The one case that plaintiffs rely on, *Calhoun v. Google, LLC*, 113 F.4th 1141 (9th Cir. 2024), undercuts their position. The defendant there argued the plaintiffs consented to the challenged data sharing because its disclosures explained the data sharing would take place. The plaintiffs disagreed, pointing out that some parts of the defendant's disclosures suggested the sharing would *not* take place, and that the defendant had a separate notice that said the sharing would not occur. *Id.* at 1147–48. The Ninth Circuit read the defendant's notice and disclosures "together" to determine the scope of the plaintiffs' consent to the defendant's conduct. *Id.* at 1149–50. Although the defendant cited *Smith*, the Ninth Circuit explained that case was "inapposite" because the plaintiffs in *Smith* had argued the scope of their consent was impacted by statements made by third parties, and not the defendant. This case, which involves the same Meta terms and policies as *Smith*, is akin to *Smith*, not *Calhoun*.

Second, plaintiffs argue they did not consent to the data sharing because Meta's terms and policies do not mention health information (Opp. 21–22), but *Smith* also rejected this argument. In *Smith*, the plaintiffs argued their consent to Meta's terms and policies did not equal consent to the collection of "health-related data due to its 'qualitatively different' and 'sensitive' nature." *Id.* at 9. The Ninth Circuit disagreed, explaining that "many other kinds of information are equally sensitive," and that "the practice complained of falls within the scope of Plaintiffs' consent to Facebook's Terms

and Policies." *Id.* In other words, the Ninth Circuit held that even assuming the information was "sensitive" in some respect, the plaintiffs nevertheless consented to Meta's collection of that information based on its terms and policies. *Id.* The same is true here, particularly because *Smith* concerned the same Meta terms and policies. The two district court cases that plaintiffs cite (Opp. 21–22), do not help them because they are contrary to the holding in *Smith* (Mot. 18).

II. Plaintiffs Cannot Prove Essential Elements Of Their CDAFA Claim.

The Court should enter summary judgment on plaintiffs' CDAFA claim for four reasons. Mot. 19–23. First, Meta did not "actively participate[]" in hacking. Plaintiffs argue otherwise, claiming it was "Meta's technology that performed the interception and Meta who ultimately uses the fruits of this unlawful activity." Opp. 23. But Meta's decision to make its SDK publicly available to app developers (subject to its terms), Flo's decision to incorporate the SDK into the Flo app, and plaintiffs' decision to download the app underscore Meta's *passive* role. Mot. 19–20.

Second, Meta did not "knowingly" "hack" anything. Plaintiffs have not pointed to any evidence even suggesting that Meta so much as directed any of Flo's or plaintiffs' actions in implementing the SDK or using the app, or even that Meta wanted health information. *See supra* 10–12.

Third, plaintiffs' consent bars their CDAFA claim—an issue addressed above.

Fourth, plaintiffs did not suffer any "damage or loss" under the statute. Plaintiffs do not dispute that none of them testified they suffered harm due to the purported loss of value of their data. Mot. 22–23. Instead, they all pointed to their own privacy interests as the source of their "harm." *Id.* Meta respectfully submits that the Court should reconsider whether an intangible privacy invasion is sufficient to establish "damage or loss" under the CDAFA, particularly given the statute's plain language and the weight of authority holding such harm insufficient under that statute. *Id.* at 21–23. The CDAFA defines "compensatory damages" to "include any expenditure reasonably and necessarily incurred by the owner . . . to verify that a computer system, computer network, computer program, or data was or was not altered, damaged, or deleted by the access." Cal. Penal Code § 502(e)(1). Plaintiffs agree that, aside from this Court's ruling on Google's summary-judgment motion, only two courts have held that the CDAFA authorizes damages for intangible invasions of privacy. Opp. 24. Plaintiffs also agree those two cases relied on *Tracking Litigation*'s discussion of Article III standing. *Id.* 24 n.15.

Given this definition, there is no reason to believe that its "damage or loss" requirement is coextensive with Article III's injury requirement. *See, e.g.*, *Heiting v. Taro Pharms. USA, Inc.*, 709 F. Supp. 3d 1007, 1021 (C.D. Cal. 2023) (agreeing with the "majority of courts" that "CDAFA's private right of action contemplates some damage to the computer system, network, program, or data contained on that computer"). The Court should grant summary judgment for Meta on plaintiffs' CDAFA claim.

III. Plaintiffs Cannot Prove Essential Elements Of Their "Aiding And Abetting" Claim.

Just as the Court held with respect to Google, plaintiffs similarly cannot prove Meta "had actual knowledge of Flo's deceptive disclosure practices," as required for their aiding-and-abetting claim. Mot. 23–25 (quoting Dkt. 485 at 5). That claim is also barred by consent. *Id.* In response, plaintiffs do not dispute they must show Meta knew about those practices. Instead, they reiterate their mischaracterizations of the record to claim there is evidence showing "Meta knew it intercepted health data" (Opp. 24), and that Meta's conduct "after the WSJ article further corroborates that Meta was a knowing participant in this intrusion" (*id.* at 24–25). Even if true, these assertions do not demonstrate Meta knew about "Flo's deceptive disclosure practices." In any event, none of this evidence actually shows what plaintiffs claim. *See supra* 10–12. If anything, their evidence shows Meta took seriously its terms' prohibitions on receiving sensitive information through the SDK. *See id.*

Plaintiffs' claims about evidence post-dating the relevant period is even less helpful for them. For example, plaintiffs claim Meta "worked directly with Flo to devise a new mechanism to continue data sharing that would avoid scrutiny from journalists" after the 2019 *WSJ* article (Opp. 24–25), but even if true, that does not demonstrate Meta knew about "Flo's deceptive disclosure practices" during the relevant period. The rest of plaintiffs' cited evidence shows only that Flo considered targeting users who were pregnant, trying to conceive, and tracking their period. *See, e.g.*, Opp. 9. The Court has already concluded such emails are "not a basis from which a reasonable jury could find aiding-and-abetting knowledge." Dkt. 485 at 6 (analyzing similar emails exchanged by Flo and Google). The Court should grant summary judgment in Meta's favor on this claim, just as it did for Google.

CONCLUSION

Because there is no genuine dispute of material fact as to any of plaintiffs' claims asserted against Meta, the Court should grant Meta's motion for summary judgment in full.

Dated: March 20, 2025

/s/ *Elizabeth K. McCloskey*

Elizabeth K. McCloskey (SBN 268184)
Abigail A. Barrera (SBN 301746)
One Embarcadero Center, Suite 2600
San Francisco, CA 94111-3715
Telephone: 415.393.8200
EMcCloskey@gibsondunn.com
ABarrera@gibsondunn.com

LATHAM & WATKINS LLP
Melanie M. Blunschi (Bar No. 234264)
melanie.blunschi@lw.com
Kristin Sheffield-Whitehead (Bar No. 304635)
kristin.whitehead@lw.com
Catherine A. Rizzoni (Bar No. 322267)
cat.rizzoni@lw.com
505 Montgomery St., Suite 2000
San Francisco, CA 94111
Telephone: +1.415.391.0600

Andrew B. Clubok (*pro hac vice*)
andrew.clubok@lw.com
555 Eleventh Street, NW, Suite 1000
Washington, D.C. 20004
Telephone: +1.202.637.2200

Michele D. Johnson (Bar No. 198298)
michele.johnson@lw.com
650 Town Center Drive, 20th Floor
Costa Mesa, CA 92626
Telephone: +1.714.540.1235

Counsel for Defendant Meta Platforms, Inc. (formerly known as Facebook, Inc.)